

ABSTRACT

[0049] Method and apparatus for providing random bits are described. In one embodiment, random bits are provided by storing a succession of random bits in a buffer. A quantity of bits is selected from the buffer at a source location and used as a basis of a new quantity of random bits. The content of the buffer is altered and the source location is advanced to the next position in the buffer. The source location is placed at the beginning of the buffer plus an offset when the next location is beyond the limit of the buffer.